软件开发包（SDK）安全与合规白皮书（2019）

CAICT 中国信通院　环球律师事务所 GLOBAL LAW OFFICE

二零一九年八月

编写团队

编写单位：

中国信息通信研究院安全研究所

北京市环球律师事务所

编写组成员：（姓氏笔画为序）

陈湉、张淑怡、孟洁、秦博阳、晏尔凡、薛颖、魏亮

版权声明

前　言

我国移动互联网市场经历了将近20年的快速发展，已经形成了庞大的产业规模，创造了可观的经济效益，并且在业务模式和商业模式创新方面引领全球。同时，移动互联网正在向传统产业加速渗透，人工智能、大数据、物联网等信息技术与实体经济持续深度融合，不断催生传统产业服务新业态，逐步改造着医疗、教育、交通、旅游、金融、传媒等传统行业的服务模式。在此过程中，移动应用软件，即App，发挥了不可替代的入口作用，全天候、全方位深度参与到了广大网民日常生活的方方面面。

App在提供各类便捷、高效、普惠服务的同时，也在无时不刻地收集、使用用户的个人信息。近年来新闻媒体曝光的涉及App个人信息保护相关事件显示，App强制授权、过度索权、超范围收集个人信息等问题已经十分突出。为此，今年1月份，中央网信办、工信部、公安部、市场监管总局四部门联合开展App违法违规收集使用个人信息专项治理，重拳出击，整治乱象。随着App个人信息保护治理工作的深入推进，与App存在密切联系的第三方软件开发包（SDK）收集个人信息问题也逐渐进入各方视野。

本报告聚焦于第三方SDK，梳理当前应用较为广泛的第三方SDK类型和市场情况，结合实际案例分析第三方SDK存在的主要安全问题

以及第三方SDK提供者与App开发者合作过程中面临的法律合规问题。通过调研欧盟、美国的相关经验做法，从法律法规、企业责任、技术标准、行业自律等方面结合我国实际情况提出了有针对性的建议。

目　录

一、第三方 SDK 的业内现状

据中国互联网络信息中心（CNNIC）统计数据显示，截止 2018 年 12 月，我国手机网民规模已达 8.17 亿，网民通过手机接入互联网的比例高达 98.6%。随着移动互联网的发展、智能手机的不断普及，移动互联网应用程序(App)得到广泛应用。据工信部统计数据显示，2018 年，我国市场上监测到的 App 总量达到 449 万款，第三方应用商店分发累计数量超过 1.8 万亿次，游戏类、系统工具类、影音播放类、社交通讯类、日常工具类、生活服务类、互联网金融类、电子商务类等 8 类 App 下载量均超过千亿次。移动互联网服务便捷、即时、普惠的特点，在 App 应用中得到充分体现，部分 App 甚至已成为广大用户生活中的“必需品”。

由于移动互联网市场的快速迭代，高科技产品飞速更新，App 开发者为了提升效率、降低成本，往往会在开发过程中嵌入第三方代码（SDK 开发包）和插件等。本章将从常见类型、应用情况、主要特点等方面对 SDK 的业内现状进行介绍，详细分析其被广泛使用的原因。

（一）第三方 SDK 常见类型及应用情况

SDK 是 Software Development Kit 的缩写，即“软件开发工具包”。简单来看，它是辅助开发某一类应用软件的相关文档、范例和工具的集合。对 App 来说，为了提高开发效率，可以将某项功能交给第三方来开发，第三方服务提供商将服务封装为工具包（即 SDK）供开发者使用。目前，SDK 类型主要包括：第三方登录分享类、支付类、推送类、广告类、数据统计分析类、地图类、风控插件以及一些基础库等。

1. 常见第三方 SDK 类型

按照第三方 SDK 能够帮助 App 开发者实现的具体功能不同进行区分，其中较为常见、与用户交互程度较强的主要有以下 6 类 SDK。

（1）第三方登录分享类

第三方登录分享类SDK主要用于简化用户登录流程，为用户使用已有的第三方帐号进行登录提供便利，同步帮助App构建自己的帐号登录体系。作为一种功能较为基础的SDK，第三方登录服务类SDK应用在各类App中广泛使用。

（2）支付类

据国家统计局2018年发布的《改革开放40年经济社会发展成就系列报告》数据显示，中国移动支付交易规模已超过81万亿元。随着移动支付的普及应用，支付功能越来越成为各类App的普遍需求。支付类SDK帮助开发者在App中进行了支付功能的集成，为用户提供购物、充值、付款、退款等相关功能。

（3）推送类

推送类SDK帮助App开发者向其用户实时推送通知或者消息，与用户保持互动，从而有效地提高用户留存率，提升用户体验。推送类SDK可实现基于用户活跃情况、设备属性、地理位置等不同用户群的推送。推送形式包括状态栏通知、自定义消息、本地通知等，内容可涵盖新闻资讯、日程提醒、活动预告、新版本更新等。

（4）广告类

据《中国互联网发展报告2018》显示，2019年网络广告市场规模将破6000

亿。随着移动广告红利时代的到来，App开始接入广告相关SDK的情形越发普遍，广告类SDK对各类广告形式的支持情况也已成为影响移动开发者收入、操作等的关键因素之一。

（5）统计分析类

数据统计分析类SDK可以帮助App开发者统计和分析流量来源、内容使用、用户属性和行为数据等，以便App开发者利用数据进行产品、运营、推广策略的决策。

（6）地图类

地图类SDK帮助App集成地图显示、交互等相关服务，以便用户在使用App时在应用中访问相关地图数据，轻松实现相关功能，并在此基础上完成基于自身场景的更深层、更个性化的开发需求。

2. 常见第三方SDK应用情况统计

为了对第三方SDK的应用情况进行进一步了解，本章节按类别梳理、总结了一些常见第三方SDK类别的应用情况[1]。

（1）第三方登录分享类

第三方登录分享类SDK主要以主流即时通讯或社交类企业推出的SDK为主，常见的类型主要有微信登录分享、微博登录分享、QQ登录分享等。嵌入此类SDK的App往往既包括App本身，也涉及App的同一母公司旗下其他产品，还包括其他各类App（如新闻资讯、视频、旅游出行等），具体情况详见表1。

[1] 相关信息梳理来自各 SDK 官网或开发者平台。

表 1：常见第三方登录分享类 SDK 应用情况统计

SDK 名称	主要业务功能	简要介绍	嵌入此类 SDK 的 App
微信登录分享	使用微信帐号快速登录第三方平台或App。	接入微信登录，实现微信帐号快速登录，一键连接。	普遍应用在各类 App 中。
微博登录分享	使用微博帐号快速登录网站或第三方 App，分享内容，同步信息。	满足了多元化移动终端用户随时随快速登录、分享信息的需求。	普遍应用在各类 App 中。
QQ 登录分享	使用 QQ 帐号快速登录网站或第三方平台。	用户使用已有的QQ号码即可登录移动应用，可减少登录交互操作，简化用户注册流程。	普遍应用在各类 App 中。

以新浪微博 SDK 为例，该 SDK 被广泛嵌入在各类 App 中，生活服务、游戏和金融行业 App 中嵌入该 SDK 的情况最为普遍，3 者合计占比 44.61%。具体分布情况如图 1 所示：

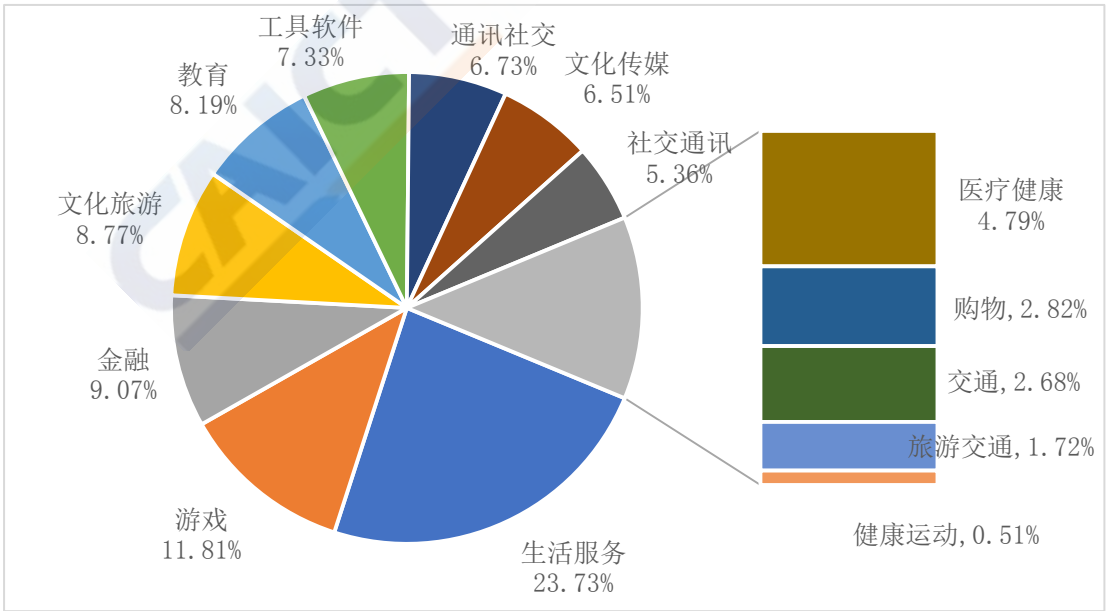


图 1 嵌入新浪微博 SDK 的 App 分布情况

（数据来源：北京智游网安科技有限公司（爱加密））

（2）支付类

支付类SDK通常提供的功能较为单一。目前常见的支付类SDK主要包括银联支付、支付宝支付、微信支付，以及各个大银行自己独有的支付SDK等。嵌入此类SDK的，除了各类电商购物平台及相关旅游出行类App外，还包括其他设置了充值、付款、退款等功能的各类App，具体情况详见表2。

表2：常见支付类SDK应用情况统计

SDK 名称	主要业务功能	简要介绍	嵌入此类 SDK 的 App
银联支付	跳转银联页面完成支付信息录入，最终完成支付。	综合性互联网支付工具，主要支持输入卡号付款、用户登录支付、网银支付、迷你付（IC 卡支付）等多种支付方式。	普遍应用在各类设置了支付场景的 App 中。
微信支付	通过点击微信付款码支付，或扫描二维码支付等功能。	综合性互联网支付工具。	普遍应用在各类设置了支付场景的 App 中。
支付宝支付	通过二维码面对面支付，小程序支付，花呗分期等多种支付功能。	综合性互联网支付工具。	普遍应用在各类设置了支付场景的 App 中。

以支付宝 SDK 为例，该 SDK 被广泛嵌入在各类设置了支付场景的 App 中，以游戏和生活服务行业最为广泛，分别有 38.85%与 24.09%的支付宝 SDK 嵌入

了该类 App。具体分布情况如图 2 所示：

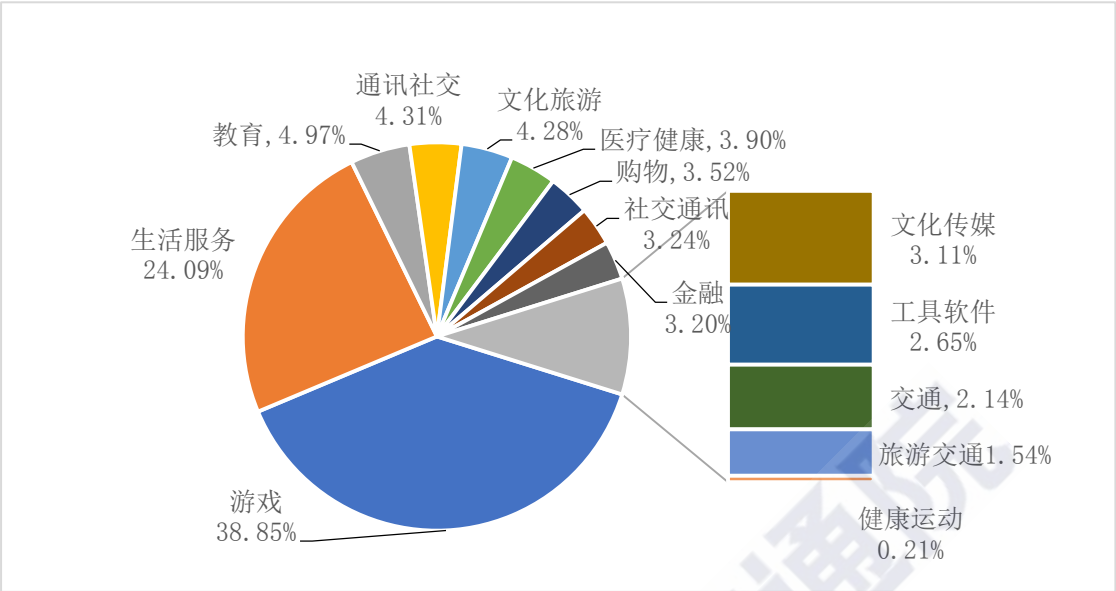


图 2 嵌入支付宝 SDK 的 App 分布情况

（数据来源：北京智游网安科技有限公司（爱加密））

（3）推送类

推送类SDK因其多强调交互式体验的特点，广泛应用于与用户互动的场景中，目前常见的推送类SDK主要有小米推送、百度云推送、个推推送、极光推送、Mob推送等。嵌入此类SDK的App包括新闻资讯、社交、地图、健康医疗、旅游出行类等App，具体情况见表3。

表3：常见推送类SDK应用情况统计

SDK 名称	主要业务功能	简要介绍	嵌入此类 SDK 的 App
小米推送	主要实现消息推送功能。	通过在云端与客户端之间建立一条稳定、可靠的长连接，为开发者提供向客户端应用实时推送	百度地图、快手、今日头条、爱奇艺、淘宝、支付宝、UC 浏览器、QQ 音乐、高德地图、拼多多、

		消息的服务，有效地帮助开发者触达用户，提升 APP 活跃度。	QQ 浏览器、滴滴出行、酷狗音乐等。
百度云推送	推送聊天消息、日程提醒、活动预告、动态、新版本更新等功能。	一站式 APP 信息推送平台，为企业和开发者提供免费的消息推送服务，开发者可以通过云推送向用户精准推送通知和自定义消息以提升用户留存率和活跃度。	手机百度、百度地图、爱奇艺、蚂蜂窝、聚美优品、我查查、虎嗅网、当当网等。
极光推送	多种消息类型、用户和推送统计、短信补充、A/B 测试、可定制的私有云等功能。	App 推送平台，每天推送消息数超过 5 亿条，应用于超过百万款 App。	工银融 e 联、中国银联、浦发银行、分期乐、融 360、翼支付、微博、探探、珍爱网、同桌游戏、去哪儿、美柚、丁香园、一起作业、京东阅读、快药、平安好医药等。
个推推送	向其用户推送各类消息，结合精准的用户画像分析，给合适的用户在合适场景下推送合适的内容。	各行业提供大数据解决方案，服务于数十万 App，覆盖数十亿移动终端	人民日报、新华社、CCTV、新浪微博、京东、网易新闻、滴滴出行等。
Mob 推送	Sharesdk、Smssdk、Moblink、Mobpush、秒验、mob 云验证	以数据应用为主导，融合大数据、云计算、人工智能等技术，SDK 下载数量超 370 万，日	绿地集团、龙珠直播、无他相机、中国电信等。

	等功能。	活用户超 2.5 亿。	

以极光推送 SDK 为例，极光推送 SDK 嵌入的 App 主要集中在金融和生活服务类 App，比例接近一半。具体分布情况如图 3 所示：

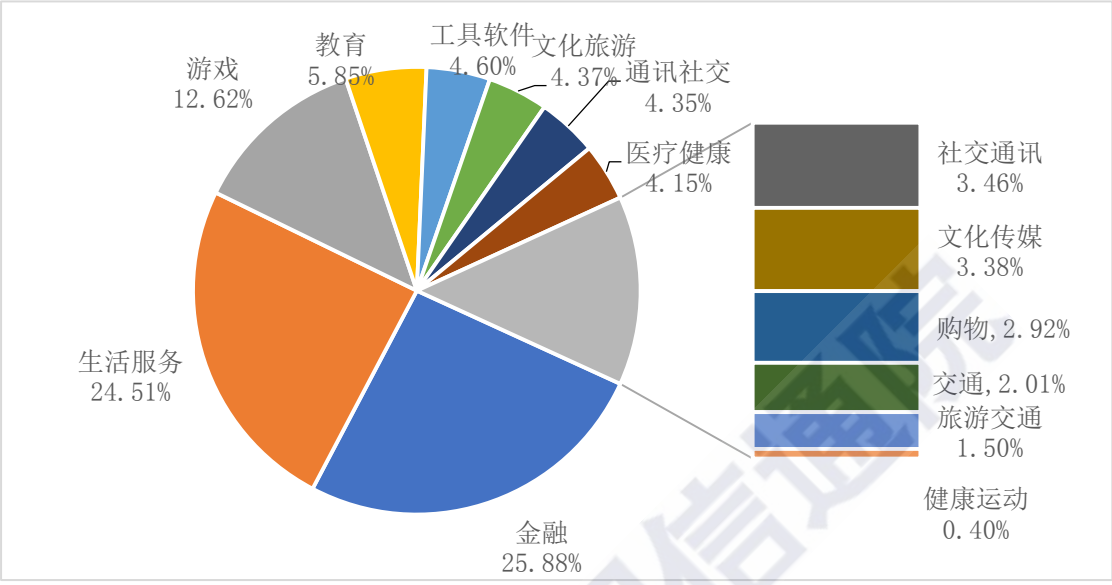


图 3 嵌入极光推送 SDK 的 App 分布情况

（数据来源：北京智游网安科技有限公司（爱加密））

（4）广告类

广告类SDK提供的服务多为程序化广告，用以实现精准营销和推广。目前，国内市场上提供移动广告相关的SDK平台众多，主流的有广点通、多盟、TalkingData、有米等。由于App普遍具有广告投放推广需求，嵌入广告类SDK的App涵盖多个类别，具体情况见表4。

表4：常见广告类SDK应用情况统计

SDK 名称	主要业务功能	简要介绍	嵌入此类 SDK 的 App
广点通	主要实现广告投放相关功能。	为 App 开发者提供广点通投放系统，通过广点通，用户可在平台多个广	欢乐淘、楚楚街、沪江教育、妈妈圈、十句话战仙、

		告位上进行应用以及应用活动相关的精准推广。	神仙道、时空猎人、美丽说等。
多盟	主要实现广告投放、营销等相关功能。	专注移动智能营销，提供程序化广告、数据营销、代理广告等服务。	中国银行、渣打银行、中国电信、招商银行、中国移动等。
TalkingData	主要实现应用统计分析、游戏运营分析、小程序统计分析等功能。	以 SmartDP 为核心的数据智能应用生态为企业赋能，帮助企业逐步实现以数据为驱动力的数字化转型。	腾讯、百度、网易、搜狐、360、Google、Yahoo 等。
有米	主要实现广告推广功能。	提供 App 推广、ASO 优化、出海营销、整合营销以及广告数据洞察等专业服务，满足游戏、电商、网服、教育、美妆等行业客户的推广需求。	封面新闻、晶报传媒、网易智造、Kappa、溢米辅导、龙之谷等。
InMobi	主要实现个性化广告功能。	全球化的移动广告平台，覆盖超过 15 亿移动设备，每月广告请求超过 2000 亿。	天使纪元、少年三国志、狂暴之翼等。

以 InMobi SDK 为例，嵌入该 SDK 的 App 中，6 成以上分布在游戏行业；其次是生活服务行业，占有 13.91%。具体分布情况如图 4 所示：

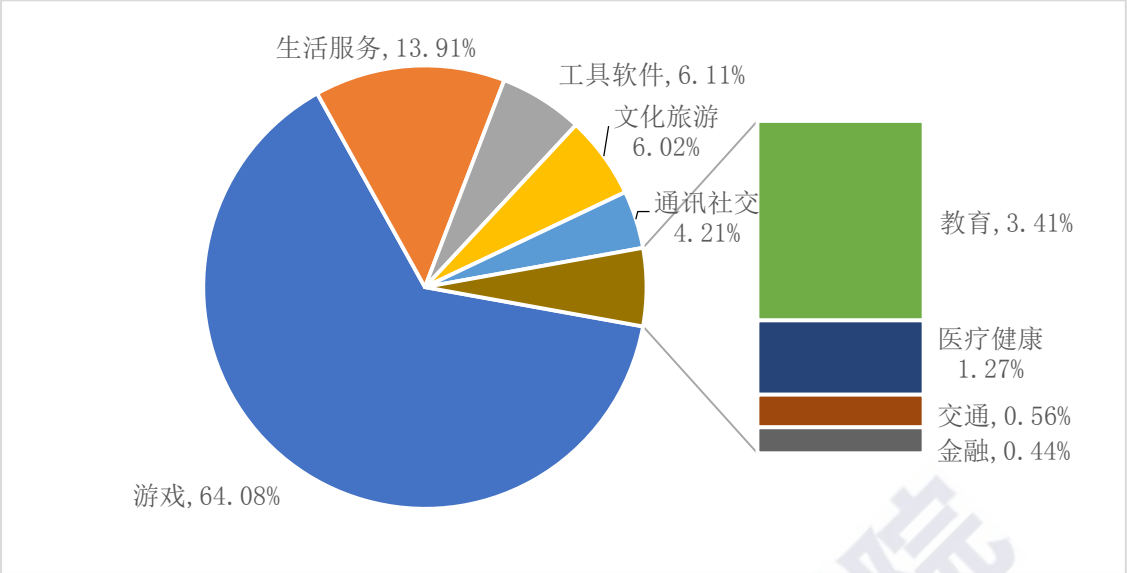


图 4 嵌入 InMobi SDK 的 App 分布情况

（数据来源：北京智游网安科技有限公司（爱加密））

（5）统计分析类

数据统计分析类SDK作为一类较不易为用户感知的SDK，对App的运营和统计分析提供支撑作用。目前，常见的数据统计分析类SDK包括友盟、海度云、贵士移动等。嵌入此类SDK的App也广泛来自各领域，且不乏各领域的头部App，具体情况见表5。

表5：常见数据分析类SDK应用情况统计

SDK 名称	主要业务功能	简要介绍	嵌入此类 SDK 的 App
友盟	主要包括移动统计、应用统计、游戏统计、移动广告监测等功能。	结合实时更新的全域数据资源，挖掘出 15,000+客群标签、输出 300+应用或行业的分析指标，通过 AI 赋能的一站式互联网数据产品与服务体系。	微博、阿里云、Kantar Worldpanel、优酷、迈外迪、酷云互动、讯码科技、云房数据、飞猪、Marketin、淘

			票票、PP 助手、钉钉、豌豆荚、掌慧纵盈等。
贵士移动	TRUTH 移动互联网标准数据库系列、TRUTH-Plus 生态流量服务、DATA MINING 数据挖掘分析服务。	帮助客户了解市场发展趋势和行业竞争格局，通过理解用户特征和全景画像优化自身运营效率，另一方面也可以帮助客户前瞻性地发现市场机会，找到具有增长潜力的赛道和值得投资的领域。	小米、百度、蚂蚁金服、中国平安、顺丰速运、腾讯、华为、苏宁易购等。
海度云	主要包括移动应用统计、网站统计、渠道分析等功能。	帮助客户了解市场发展趋势和行业竞争格局，优化自身运营效率，帮助客户发现市场机会，日接受移动数据量超过 150 亿。	YY、ME 直播、100 教育、环球网校、无忧英语、邢帅教育、闲趣网络等。

（6）地图类

地图类 SDK 帮助开发者实现地图数据的调用及相关服务的实现。目前，常见地图类 SDK 主要包括百度地图、高德地图、腾讯地图等。嵌入此类 SDK 的 App 多为旅游出行、电商购物、物流、外卖等，具体情况见表 6。

表 6：常见地图类 SDK 应用情况统计

SDK 名称	主要业务功能	简要介绍	嵌入此类 SDK 的 App
百度地图	主要有地图、定位、搜索、轨迹、导航、路线规划、路况等功能。	提供手机端、PC 端、智能穿戴设备的地图展示能力，在多个行业场景中可以配置个	摩拜单车、e 袋洗、点到、德邦、苏宁易购、货拉拉、

		性的地图展示效果。	唯品会等。
高德地图	主要有地图、定位、导航、路线规划、搜索、自定义地图和数据可视化等功能。	LBS 服务提供商，服务超过三十万款移动应用，日均处理定位请求及路径规划数百亿次。	首汽约车、易到、神州专车、曹操专车、嘀嗒出行、饿了么等。
腾讯地图	主要有定位、地图展示、地点搜索、路线规划、导航和室内图等功能。	基于 Android 4.1 及以上版本设备的应用程序接口，通过该接口，可以轻松的使用腾讯地图定位服务。	京东、中国邮政、新达达、汇通天下、滴滴出行、美团外卖、快手等。

3.第三方 SDK的应用特点分析

从第三方SDK应用情况来看，主要呈现以下三个特点：

一是App使用第三方SDK已成为普遍现象。根据爱加密大数据中心提供的数据，截至2019年4月底，在其收录的共计约267万条Android应用数据中，超50%的App都不同程度地使用了第三方公司提供的SDK工具包。可以说，SDK已成为与App相生相依的重要伙伴，也同时成为了整个移动互联网生态中极其关键的一环。

二是各类别App平均使用第三方SDK的数量在10个以上。随着第三方SDK种类及数量的不断增多，不少App开发者由于开发时间和成本有限，大量使用第三方SDK进行代码集成。如图2所示，根据CSDN社区专业人士利用SDK分析工具，针对1000多款主流App使用SDK情况得出的统计数据[2]，各类别App使用第三方SDK平均在10个以上，最高可达平均30.6个/类。平均使用第三方SDK个数超过20

[2] https://blog.csdn.net/rohsuton/article/details/78022158，最后访问时间 2019 年 7 月 20 日。

个的App类型有8类。

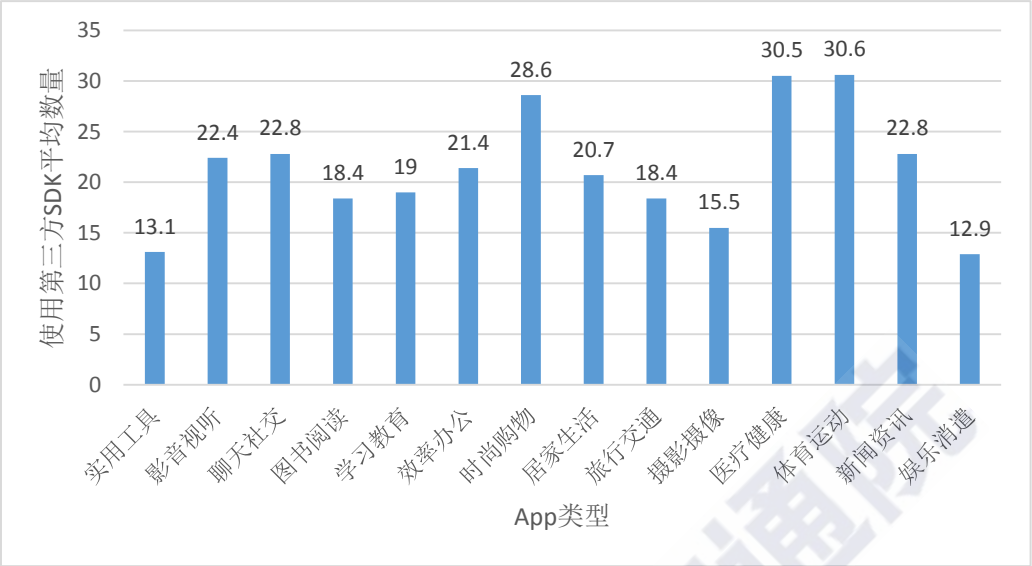


图5　App中使用第三方SDK的数量分布图

（数据来源：CSDN“IT东”博客的SDK分析工具）

三是第三方SDK功能逐渐多样化，应用于不同领域的大量App中。目前，市场上的第三方SDK提供者已不再局限于开发功能单一的SDK，而是将SDK功能从纵向和横向不断延伸，从而应用于不同领域的大量App中。以推送类SDK提供者为例，除了不断完善基于用户画像的实时、智能、多场景下的精准推送外，往往会同步对产品运营情况进行统计分析，帮助App进行产品优化升级，甚至部分SDK提供者还同步推出了登录验证功能。随着第三方SDK功能的不断强大并逐渐多样化，其应用市场的规模将持续扩大，市场前景持续看好。可以说，第三方SDK已成为事实上链接各类业务功能App的数据枢纽，有机会获取来自各类App不同业务场景下多类别的个人信息。

（二）第三方 SDK 普遍应用的原因分析

一是接入第三方 SDK 可以大幅度提升使用者的开发效率，明显降低开发成本。特别是推送类、广告类等 SDK，往往能够帮助 App 开发者在无需了解技术细节的情况下快速实现某一特定功能，从而提高开发效率，缩短开发周期。这样，App 开发者也可以将精力放在商业模式的制定与运营上，提高整体效率。

二是 SDK 的易用性和灵活性较强，为 App 提供流畅及定制化的用户体验。SDK 通过创造一种简单的模式，简化代码、优化繁琐的集成工作，实现 API 的有效调用，配置简便、友好、灵活。在实际中，开发者的需求各异，可以通过集成不同类型的 SDK 快速实现预期功能，构建自定义应用，并为其用户量身定制体验，大大增加应用程序的多样性，提高 App 的用户留存率和使用频率。

三是 SDK 能够帮助提高 App 的兼容性，扩大用户使用范围。SDK 的接入可以解决 App 具体功能与各厂商机型的兼容性问题，免去与各厂商机型繁琐的硬件适配工作，让使用各种机型的用户都能够使用 App 的某一特定功能，解决 App 在各应用市场的投放中可能存在的渠道兼容问题。

二、第三方 SDK 的主要安全问题及分析

随着四部门 App 违法违规收集使用个人信息专项治理行动的持续深入推进，原本“隐藏”在 App 身后的第三方 SDK 进入了监管部门及公众视野，其目前存在的一些安全风险及收集使用个人信息的合规问题，也随之浮出水面。

（一）第三方 SDK 自身安全性不容乐观

目前，已经发现的 SDK 安全漏洞包括 http 误用、SSL/TLS 不正确配置、敏感权限滥用、身份识别、本地服务、通过日志造成信息泄露、开发人员失误等[3]。第三方 SDK 的应用模式决定了其自身安全问题往往产生放大效应，嵌入第三方 SDK 的 App 越多，其安全漏洞的波及范围就越广，严重时甚至能够影响 Android 生态系统安全。以 2017 年 12 月爆出的某消息推送类 SDK 漏洞为例，因其存在可越权调用未导出组件漏洞，利用该漏洞便可实现对嵌入了该 SDK 的 App 进行多种恶意攻击，包括远程窃取用户终端设备中的敏感数据（通讯录、照片、账号密码等）、向终端用户推送虚假诈骗信息等。据悉，该漏洞共影响了七千多款 App[4]，其中不乏市场主流产品，影响范围极广。

（二）第三方 SDK 成为病毒传播新途径

当前，App 普遍使用第三方 SDK 的现象也吸引了一些不法分子的注意。通过制作、发布、吸引 App 嵌入含有恶意代码的第三方 SDK，造成短时间、大范围的病毒传播和感染；并且使用代码分离、动态代码加载等技术，能够实现远程控制恶意代码的执行，具有很强的隐蔽性和对抗杀毒软件的能力。2018 年 4 月，腾讯安全反诈实验室曝光了一款推送类的恶意第三方 SDK——“寄生推”，它通过预留“后门”，云端动态更新下发恶意代码包，对感染手机进行 Root 提权，静默安装恶意应用，推送恶意广告，牟取不法收益。“寄生推”采用的云端控制下发恶意代码的方式，绕过了一些应用市场的 App 安装包检测和杀毒软件的蜜

[3] 马凯，郭山清. 面向 Android 生态系统中的第三方 SDK 安全性分析[J]. 软件学报, 2018, v.29(05):207-219.

[4] http://www.freebuf.com/articles/system/156332.html，最后访问时间 2019 年 7 月 23 日。

罐检测。据腾讯统计，共有 300 多款 App 嵌入了“寄生推”，潜在受影响用户数超 2000 万。

（三）第三方 SDK 隐蔽收集个人信息问题逐步显现

第三方 SDK 作为独立的软件开发工具包，和 App 一样，具备收集个人信息的能力。但第三方 SDK 收集了哪些个人信息，用户往往难以感知，App 开发者也未必完全知悉。今年以来，已经发生多起第三方 SDK 隐蔽收集个人信息的安全事件。例如，2019 年 2 月《华尔街日报》曝光 Facebook 在未告知用户的情况下，利用 App Events 统计分析工具从 11 个应用程序中收集用户个人敏感信息。此前，卡巴斯基实验室研究人员 Roman Unuchek 也曾披露，某些第三方 SDK 会主动收集用户姓名、年龄、性别、电话号码、邮箱地址、位置信息、设备信息等众多个人信息和个人敏感信息，并以明文方式上传至远程服务器，且不论用户是否知情同意，明文传输本身已经加剧了个人信息的泄露风险[5]。

三、第三方 SDK 的主要合规问题及分析

本章将主要讨论聚焦于第三方 SDK 收集使用个人信息在法律层面的合规问题，有别于上一章关于第三方 SDK 隐蔽收集个人信息的安全问题。对于第三方 SDK 被普遍使用、大量获取个人信息的现状形成鲜明对比的是，第三方 SDK 的个人信息收集使用行为经常缺少法律层面的正当性，因此存在合规风险。这些合规风险的产生，因第三方 SDK 提供者在用户和 App 关系中起到的角色不同—在 App“背后”处理数据或通过 App 接入、以自己名义提供服务—而有所差异。

[5] http://www.sohu.com/a/228862055_100066938，最后访问时间 2019 年 7 月 23 日。

（一）第三方 SDK 作为数据处理者时，主要合规问题分析

在某种情况下，App 终端用户在使用 App 服务过程中虽然会被 SDK 直接收集个人信息，但用户自身对这类 SDK 的存在是无感知的，例如终端用户在使用 App 内的语音通话功能时被嵌入该 App 的语音分析 SDK 收集语音信息，用户是无法知悉其个人信息被哪个语音 SDK 提供者收集、使用和存储了。

如果 App 与第三方 SDK 之间约定，App 开发者是数据控制者，第三方 SDK 提供者是受 App 委托的数据处理者，那么在私法层面上第三方 SDK 提供者将无法与用户直接建立“合同”关系，也就无法以自己的名义就收集使用用户个人信息的行为获得个人信息主体的同意。此时，第三方 SDK 提供者收集使用个人信息的正当性依据来自于：（a）App 开发者就该等数据的收集、使用和“分享”获得用户的同意；以及（b）App 开发者给予的委托处理数据之授权，条件（a）和（b）缺一不可。

然而，现实情况是，第三方 SDK 所收集和使用的个人信息及相关共享行为，很多 App 开发者并没有通过隐私政策或弹窗提示等方式获得用户的“同意”，显然也就无法满足（a）项条件；同时，为满足 App 的便利、便捷开发需求，第三方 SDK 提供者与 App 开发者往往通过第三方 SDK 提供者的开放平台，在线签署开发者服务协议来约定双方的权利义务，鲜少有关于委托处理数据方面的专门协议或特别规定，也就难以算作协议双方之间的有效“授权”，（b）项条件也未必满足。此外，目前大多数 App 开发者不会对第三方 SDK 收集了那些个人信息进行技术验证， 此种情况下的第三方 SDK 的数据收集和处理活动对于 App 开发者而言相当于一个“黑盒子”，缺乏透明度，如果被诉侵犯个人用户隐私的，

App 开发者或者 SDK 提供者将可能承担举证责任倒置的风险。[6]

（二）第三方 SDK 作为共同数据控制者时，主要合规问题分析

在某些情况下，接入应用的 SDK 是以自己的名义向 App 的用户提供服务的，比如 App 用户通过激活一个 SDK 接口而调用或者启动了该用户已安装的另一个 App 的服务功能。此时，第三方 SDK 提供者能够拥有独立的“数据控制者”身份，因为第三方 SDK 提供者有机会将自身品牌进行露出，用户对其使用的是哪家企业实际提供的特定服务是有明显感知的。采用三重授权原则，即“【用户-平台 1】+ 【平台 1-平台 2】+ 【用户-平台 2】”可以解决正当性问题。但是如果第三方 SDK 提供者在“同意”范围之外处理用户个人信息的，则该等数据处理的行为则显然不具备法律正当性，需要承担超出授权范围的相关责任。

现实情况中，也有少数第三方 SDK 提供者在 App 开发者合作委托其处理数据时，也坚持要求获得“共同数据控制者”身份，以此确保自身对数据使用目的、方式的“自主权”，并且在获取后也不会根据 App 开发者的指令进行销毁或者交还数据。其背后的动力来源于第三方 SDK 提供者汇聚多源数据后，更需要能够自主决定如何处理数据，进而实现数据变现。

即使第三方 SDK 有可能变成“共同控制者”的身份，由于第三方 SDK 依然不直接面对用户，需要 App 开发者提供代为告知用户（如增加告知链接、弹窗告知变更隐私政策等）并获得用户“同意”，会增加 App 开发者的运营成本，

[6] 例如在庞理鹏诉北京趣拿信息技术有限公司、中国东方航空股份有限公司案件中，被告东航主张其通过与中航信签订《航空公司服务协议》，委托中航信为东航提供民航商务数据网络服务。由于原告（个体消费者）无法也没有能力拿到相关证据证明其个人信息是东航或趣拿公司泄露的，二审法院认为原告提供的证据已经足以表明其完成了“高度可能泄露”的举证责任，被告如果无法举证证明其不存在泄露庞理鹏个人隐私信息的，被告应该承担赔偿责任。因此，该案其实适用了举证责任倒置。

多次弹窗还会影响用户体验。App 开发者还需要基于合同相对性，针对第三方 SDK 收集使用用户个人信息的情况，对用户承担合同法下的违约责任以及网络安全法下的行政责任，同时还有义务将各项合规义务传导至第三方 SDK 提供者。

四、第三方 SDK 管理的域外经验

（一）欧盟的第三方 SDK 管理经验

欧盟背景下对第三方 SDK 提供者收集、处理用户个人信息的行为是通过欧盟《通用数据保护条例》（General Data Protection Regulation,以下简称“GDPR”）进行规制的。[7]

1. 第三方 SDK 提供者在 GDPR 中的定位既可能是数据控制者也可能是数据处理者

现实中，根据 SafeDK 调研 190000 个 App 后发布的《2018 SDK 数据使用趋势年度报告》的统计数据，SDK 会通过调用 App 提供的数据，对用户个人信息（包括位置信息、联系方式、账户名称，见图 6）进行收集、缓存并上报至 SDK 服务端，即 SDK 提供者的行为构成对数据的收集和处理并应受到 GDPR 的规制。

[7] 根据 GDPR 第 4（1）条的定义，“个人数据”是指任何已识别或可识别的自然人的相关信息，包括姓名、地理位置数据等。任何对该等数据的收集或处理均受到 GDPR 的规制。

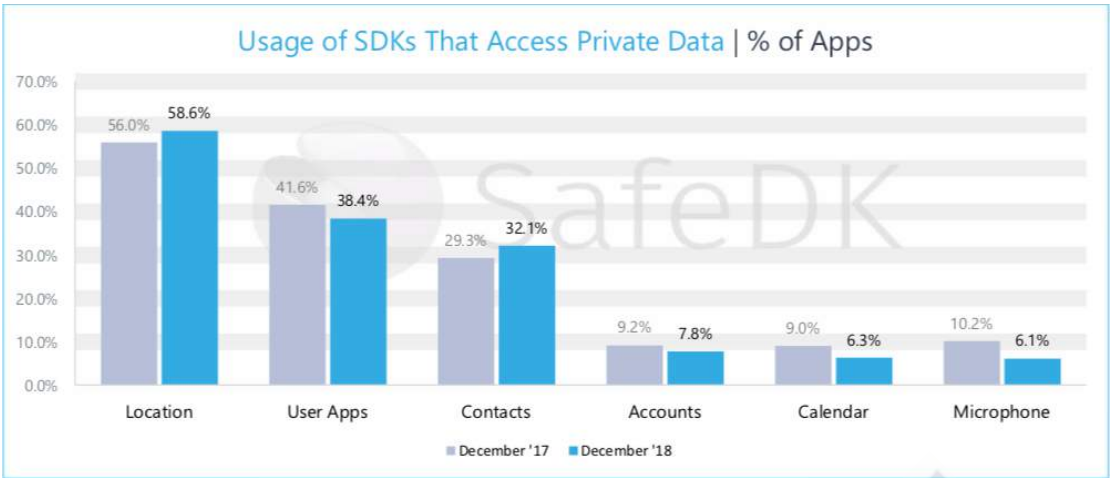


图 6 SDK 通过 App 收集的数据类型统计

（来源：SafeDK – 2018 SDK 数据使用趋势年度报告）

GDPR 对于数据处理的义务与责任问题是通过各方在具体数据处理中担任的角色 – 数据控制者、数据处理者 – 来分配的。根据 GDPR 第 4 条的定义，数据控制者是指决定处理个人信息的目的和方式的自然人、法人、公共机构或者其他机构，数据控制者可以为多个。数据处理者是指代数据控制者处理个人数据的自然人、法人、公共机构或者其他机构。

在 App-SDK 关系中，App 开发者是数据控制者以及处理用户个人数据的首要责任人，SDK 提供者是 App 分享数据的第三方（即数据处理者）；也有可能 App 开发者与第三方 SDK 提供者均是以自己名义自行决定处理数据的目的与方式的数据控制者。第三方 SDK 提供者具体担任什么角色需要在个案中进行分析。

例如，欧洲法院在 2019 年 7 月 29 日发布的 Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV 一案的指导建议中表示，网站运营商在其网站上嵌入 Facebook 的点赞按钮，并将访问者个人数据收集、传输给 Facebook，可能与 Facebook 一同构成数据的共同控制者，网站运营商原则上对 Facebook 之后对个人数据的单独处理行为不承担控制者的责任。

本案中的数据的收集和处理进程可以分为两个阶段：其一，Fashion ID 收集并传输给 Facebook 的阶段；其二，传输后由 Facebook 独立处理数据的阶段。就第一个阶段而言，Fashion ID 和 Facebook 共同决定了数据收集和处理的目的和方式（待德国杜鲁尔多夫高级地区法院进一步调查后确定相关细节），因此可以认定 Fashion ID 就本案中第一阶段的数据收集和传输行为与 Facebook 一同构成共同控制者。

根据 GDPR 的规定，不论第三方 SDK 提供者担任的是何种角色，其在个人数据的收集或处理之前，应取得 GDPR 第 6 条规定的处理个人数据的合法依据，并且，处理数据时应符合 GDPR 第 5 条规定的基本原则等要求。

（1）第三方 SDK 提供者处理个人数据前需获得数据主体的同意

GDPR 第 6 条第（1）款规定的处理的合法依据包括：

“只有满足至少如下一项条件时，处理才是合法的，且处理的合法性只限于满足条件内的处理：

（a）数据主体已经同意基于一个或多个特定目的而对其个人数据进行处理；

（b）处理对于履行某项数据主体为当事人的合同是必要的，或者在签订合同前基于数据主体的请求而进行的处理；

（c）处理是为履行其法定义务所必需的；

（d）处理对于保护数据主体或另一个自然人的核心利益所必要的；

（e）处理是数据控制者为了公共利益或应官方机关要求而进行的；

（f）处理对于控制者或第三方所追求的正当利益是必要的，这不包括需要通过个人数据保护以实现数据主体的优先性利益或基本权利与自由，特别是儿童的优先性利益或基本权利与自由。”

此外，如果处理的数据涉及 GDPR 第 9 条规定的敏感数据（包括有关种族、宗教、政治观念、为识别特定自然人的基因、生物数据），则必须获得数据主体的明示同意。

如本报告第一章所介绍的，第三方 SDK 提供者收集、使用个人数据是为了提高自身或者 App 的服务，而非（b）-（f） 项规定的特殊情况。换言之，如果第三方 SDK 确有处理数据的行为，则只能根据第（a）项，即获得用户的同意。GDPR 在第 4（11）和 7 条规定了“同意”的构成要件：“自由做出、特定、知悉、不含混”，即告知用户哪些信息将被处理，被谁处理，以及基于什么目的被处理，且不得采取默认同意的方式。

（2）第三方 SDK 获得用户同意的方式

因为第三方 SDK 集成于 App 中，面对用户、更直接向其提供服务的是 App，而非第三方 SDK，故第三方 SDK 提供者想要获得用户同意无法绕开 App，只能通过 App 才能进行。在这种情况下，获取用户同意对内可以分三步来完成：

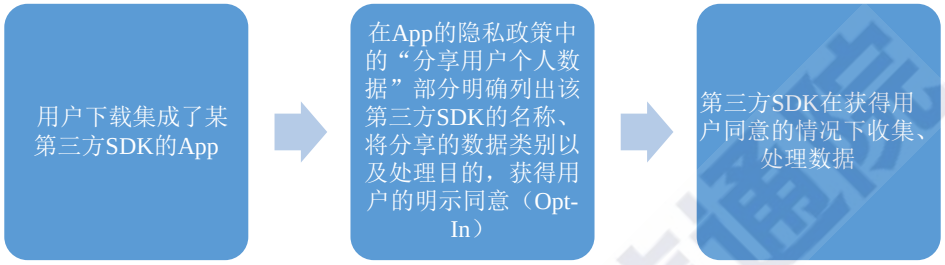
第一步：第三方 SDK 提供者告知 App 开发者 SDK 将要处理用户哪些个人信息；

第二步：App 开发者在隐私政策的“与第三方分享数据”一节中说明，哪些数据将由第三方 SDK 提供者收集，或者哪些数据类型是由 App 共享给第三方 SDK 提供者以及该等处理的目的；或通过在 App 的隐私政策中跳出 SDK 隐私声明的链接，由 SDK 发布单独的隐私声明来获取用户的同意；

第三步：第三方 SDK 通过 App 获得用户对 SDK 处理数据的同意。

以下通过图例将第三方 SDK 获取用户同意的三个步骤更清晰、直观地进行描述：

对外呈现的形式为：



2. 第三方 SDK 提供者未获得用户同意收集数据将受到监管处罚

就监管机构设置而言，整体上，由欧盟数据保护委员会（European Data Protection Board, “EDPB”）制定指南性文件，确保 GDPR 在欧盟各国执法的统一性，协调各国数据保护机构，作为最高裁决者对涉及多国争议发布具有拘束力的决定；就各个国家而言，由各国设立的独立数据保护监管机构（DPA）依据 GDPR 对违规企业进行执法，例如英国信息专员办公室（Information Commissioner’s Office, “ICO”），法国信息监管委员会（Commission Nationale de l’Informatique, “CNIL”）等。因此，如果第三方 SDK 提供者未经用户同意自行处理用户个人数据，第三方 SDK 提供者将可能因违反 GDPR 第 6 条处理须有合法依据以及第 5 条规定的数据处理的合法性、透明性而承担法律责任，由各国的 DPA 进行执法，而 EDPB 可能会基于“一致性”原则进行统一协调。

（二）美国的第三方 SDK 管理经验

美国在联邦层面没有统一的个人信息保护法，而是呈现出行业化和各州分散立法的特点，如 1914 年针对损害消费者利益的商业行为颁布《联邦贸易委员会法案》[8]、1996 年颁布的《健康保险流通与责任法案》、1998 年针对未满 13 周岁的美国公民颁布的《儿童在线隐私保护法案》、1999 年颁布的《金融服务现代化法案》等。2018 年 6 月颁布的《加州消费者隐私保护法案》（California Consumer Privacy Act，以下简称“CCPA”），从州层面上体现了民众对保护个人隐私的重视以及美国关于个人数据保护的一些最新理念。鉴于 CCPA 在美国有较大的影响力和代表性，以下将以 CCPA 为例，进行重点分析。

1. 第三方 SDK 提供者在 CCPA 的定位是收集或代为收集，并自行或与他人共同决定处理目的的“企业”

与 GDPR 不同，CCPA 并未区分数据控制者或数据处理者。根据 CCPA 第 1798.140(c)的规定，只要第三方 SDK 提供者收集或代为收集消费者个人信息，并自行或与他人共同决定个人信息的处理目的，且满足年总收入超过 2500 万美元，或为商业目的购买、出售、分享超过 50000 条消费者、家庭或设备的个人信息，或通过销售消费者个人信息取得的年收入超过总收入的 50%，即为受到 CCPA 规制的“企业”，承担相应的义务并履行相应的责任。

CCPA 对于个人信息（personal information）的定义比 GDPR 的个人数据（personal data）更为广泛，是指能够直接或间接识别、描述与特定的消费者或其家庭相关或合理相关的信息。但与 GDPR 对处理任何个人数据均需要获得明

[8] 1938 年《惠勒—利法》、1950 年《塞勒—凯弗维尔法》和 1980 年《反托拉斯诉讼程序改进法》对《联邦贸易委员会法》第 5 条、第 7 条进行修改。

示同意（Opt-In）不同，CCPA 对个人信息的出售、披露进行规制，且采用的是以 Opt-Out 为主、Opt-In 为辅的模式。

（1）第三方 SDK 提供者收集消费者个人信息只需要告知，无需获得同意

在 Opt-Out 机制下收集个人信息无需事先征得用户的同意只需要告知[9]，但在后续出售个人信息过程中需要让用户完全知情（透明性）以及给予用户更多的选择权（可控性）比如行使拒绝的权利。因此，第三方 SDK 提供者在收集个人信息前或收集时应当告知（inform）个人信息主体其所收集的个人信息的类别、内容和使用目的，但无需征得个人信息主体的明示同意。

（2）SDK 提供者向第三方出售个人信息需向消费者提供免于其个人信息被出售的选择退出权

CCPA 第 1798.120（a）规定："消费者有权在任何时候指示一个拟将其个人信息出售的第三方，不得出售其个人信息"。因此，当存在 SDK 提供者出售消费者的个人信息时，CCPA 赋予消费者拒绝的权利（Opt-Out）。SDK 提供者在收到消费者的指示起即不得再出售该消费者的个人信息 ,除非随后得到该消费者就其个人信息出售的明示授权。

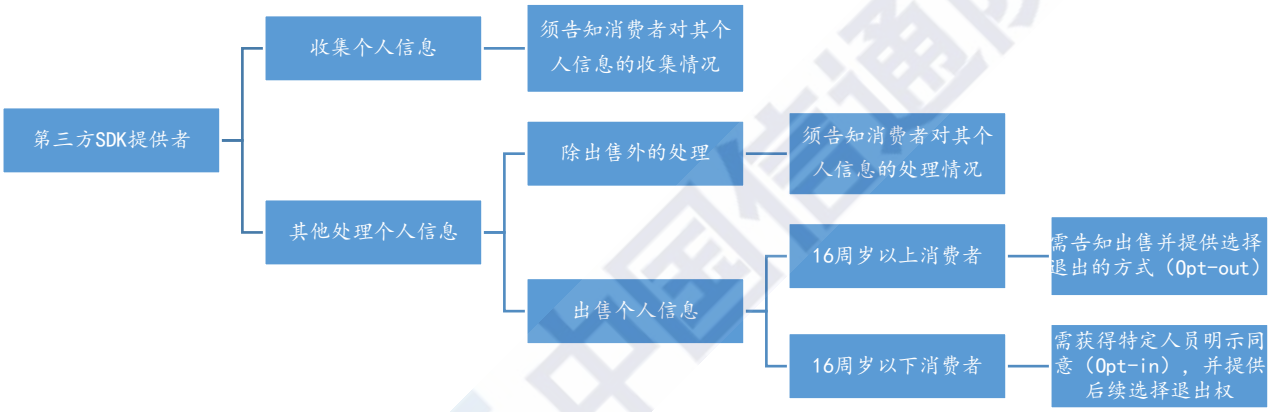
（3）第三方 SDK 提供者出售 16 周岁以下消费者的个人信息前需获得明示同意

对于 16 周岁以下消费者个人信息的出售，CCPA 采取的是获得特定人员明

[9] CCPA 第 1798.100（b）规定："收集消费者个人信息的企业应当在收集时或者收集前告知消费者所收集个人信息的类别以及个人信息的使用目的。在未向消费者提供符合本节要求的告知情况下，企业不得收集其他类别的个人信息，或者将所收集个人信息用于其他目的。"

示同意（Opt-In）的模式，即企业有请求用户明示授权的义务。[10] 故在 App-SDK 场景下，对于 16 周岁（含）以上的用户，第三方 SDK 提供者仅需通过 App 告知用户将要出售其个人信息，并在后续出售信息时提供用户拒绝的方式即可，但对于 16 周岁以下的用户，则需要取得法案所规定人员的明示授权才能出售其个人信息。

以下通过图例将 CCPA 规定的告知义务和获得同意的义务更清晰、直观地进行描述：



（4）第三方 SDK 提供者告知以及获得同意的方式

如前所述，第三方 SDK 提供者想要告知或就出售行为获得特定消费者同意无法绕开 App，只能通过 App 来进行。在这种情况下，对内也需分三步来完成：

第一步：第三方 SDK 提供者告知 App 开发者 SDK 将要收集、处理消费者的哪些个人信息；

第二步：App 开发者在隐私政策的“与第三方分享个人信息”一节中告知或

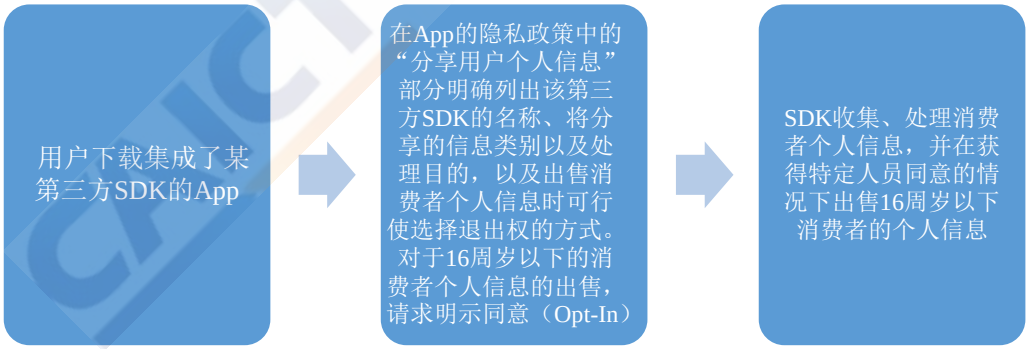
[10] CCPA 第 1798.120（d）项规定，“尽管有第（a）项规定，如果企业明知消费者年龄小于 16 岁，企业不应出售该消费者的个人信息，除非在 13 至 16 岁之间的消费者明示授权，或年龄小于 13 岁消费者的父母或监护人明示授权企业可以出售该消费者个人信息。企业任何故意忽视消费者年龄的行为应被视为其已明确知晓该消费者年龄。”

通过在 App 的隐私政策中跳出 SDK 隐私声明的链接，由 SDK 发布单独的隐私声明来告知哪些个人信息将会由第三方 SDK 提供者收集，或者哪些信息类型是由 App 共享给第三方 SDK 提供者以及该等处理的目的。

第三步：如涉及消费者个人信息的出售，则需要明确告知消费者的选择退出权和行使方式，如特别涉及 16 周岁以下消费者个人信息出售，则须在出售前获得 CCPA 规定的特定人员的明示同意。

以下通过图例将 SDK 获取用户同意的三个步骤更清晰、直观地进行描述：

对外呈现的形式为：



2. 第三方 SDK 提供者未履行告知义务、就出售未提供选择退出权或获得特定人员同意将受到监管处罚

就监管机构设置而言，对第三方 SDK 提供者的规制是联邦层面和州层面双轨监督体系。在联邦层面，主要由联邦贸易委员会（Federal Trade Commission，“FTC”）依据《联邦贸易委员会法案》对离线和在线侵犯消费者隐私和数据安

全问题进行概括监管；同时对其制定的《儿童在线隐私保护法案》等法案进行执法。在州层面，由各州的执法机构根据各州隐私保护法案（如有）进行执法，例如加利福尼亚州司法部（California Department of Justice）根据 CCPA 对相关企业进行执法。因此，如果第三方 SDK 提供者未履行告知义务、就出售消费者个人信息未提供选择退出权或获得特定人员同意，将会受到 FTC 根据联邦部门法，以及州司法部根据州隐私法案的双轨监管处罚。

五、针对我国第三方 SDK 管理的相关建议

本报告通过分析第三方 SDK 存在的安全问题和法律合规问题，结合国外管理经验和实践做法，提出如下建议：

（一）尽快完善相关法律法规，明确相关主体的责任义务

建议在《中华人民共和国网络安全法》和《中华人民共和国电子商务法》等现行法律法规中补充与第三方 SDK 相关的规定，并在已经列入立法规划的《个人信息保护法》或正在公开征求意见的《数据安全管理办法（征求意见稿）》和《网络安全审查办法（征求意见稿）》等行政规章中对第三方 SDK 进行关注，并明确 App 开发者和第三方 SDK 提供者各自的义务和责任。特别对于《数据安全管理办法（征求意见稿）》第三十条，建议明确包含 App 嵌入第三方 SDK 的情况，否则对于目前表述“接入其平台的第三方应用”，有可能会被理解为仅涉及平台与第三方应用之间的关系，不涉及第三方 SDK。

参考国外实践，建议在法律法规中明确要求 App 开发者与第三方 SDK 提供者等网络运营者在获取、共享、使用用户个人信息时，需有具体的、清晰的和正

当的目的，给予用户知情权和控制权，并且获得用户的同意；明确 App 开发者和第三方 SDK 提供者分别的法律义务与责任，如 App 开发者作为网络运营者需对第三方 SDK 提供者数据请求的必要性进行评估，并且可以拒绝不必要的个人信息请求，在发现超出约定行为时及时采取措施，对第三方 SDK 提供者数据安全管理情况进行必要监督等。另外，建议在法律法规中引入惩罚条款，对 App 开发者超出 SDK 提供者的请求范围提供个人信息，以及 SDK 提供者超出授权范围和使用目的收集使用个人信息的行为进行处罚。

（二）App 开发者需要积极履行数据共享合规义务

一是完善隐私政策，清晰告知收集个人信息情况并获取用户同意。App 的隐私政策需明确告知用户 App 接入了哪些 SDK，这些 SDK 可能会收集、使用用户哪些个人信息，并明确收集、使用个人信息的目的以及必要性，并且获得用户的明确授权。如将所有第三方 SDK 提供者的名称全部列全确实存在困难，至少需要说明第三方服务提供方的类型，并且提供退出路径可供用户选择（Opt-Out）。

二是完善合作协议，明确约定第三方 SDK 提供者能够直接采集或 App 共享的个人信息清单。清单内容包括但不限于收集信息的目的、方式、范围、数量和存储时间。App 开发者承担评估第三方 SDK 提供者收集个人信息清单中所列信息必要性的责任。当且仅当用户明确、自由地表达同意后，该用户个人信息才可以被收集或共享给第三方 SDK 提供者。否则，第三方 SDK 提供者需要承担未经授权或者超出授权同意而收集使用用户个人信息的责任。

三是强化第三方 SDK 收集、使用个人信息活动的安全管理。App 对合作第三方 SDK 的安全管理体现在事前审核、事中监督、事后保障三个环节。事前审

核，即在建立合作关系时、供应商入库环节中增加安全及合规审核，以及对第三方 SDK 提供者的尽职调查与数据安全能力评估；事中监督，是指在合作过程中如发现第三方 SDK 违规调取用户个人信息、出售用户个人信息的情况需要及时处置，落实惩罚机制；事后保障，即在合作后期或合作终止但用户个人信息尚未被处置前，App 开发者仍需保障个人数据安全的连带义务和责任。此外，合作过程中，建议 App 开发者针对不同类型的第三方 SDK 提供者，建立 SDK 收集、使用个人信息活动的评估机制，定期对第三方 SDK 提供者进行数据安全保护能力鉴定。评估机制从技术方法上应重点关注 SDK 收集、使用个人信息范围的必要性、数量与评估 SDK 所收集的用户个人信息和向自己所提供服务的关联程度，对于与服务功能无关的收集和使用个人信息的类型，建议予以取消授权，并视严重情况终止与其合作。

四是定期对第三方 SDK 提供者的数据安全保障能力进行审计。建议 App 开发者指定独立的数据安全审计员或者第三方专业机构对第三方 SDK 提供者的数据安全保障能力进行定期检查，如是否采取完备的安全措施（如加密、脱敏、分类分级等）以保障数据处理过程中的安全性；是否建立严格的数据访问权限管理机制，降低人为泄密的风险；是否对数据处理活动进行记录，以检测不当访问处理数据的行为等。

（三）第三方 SDK 提供者需要加快构建数据安全合规体系

一是制定、公开个人信息收集使用规则。从前述分析来看，第三方 SDK 提供者不论作为数据控制者，还是作为数据处理者，都需要向 App 开发者及最终用户公开其个人信息收集使用规则，具体形式可以是除 App 开发者的隐私政策

说明以外，在自己的网站或者开放平台中放置隐私政策。在隐私政策中，第三方SDK 提供者需要准确说明其提供的 SDK 提供的功能，每类功能对应收集的个人信息类型，以及收集、使用个人信息的具体目的、方式、范围。关于隐私政策的具体要求，可以参考《GB/T35273-2017 信息安全技术 个人信息安全规范》。

二是加强与 App 开发者合作数据合规管理。第三方 SDK 提供者作为数据处理者或共同数据控制者时，需要依赖 App 开发者获得收集、使用个人信息的法律正当性事由。为此，第三方 SDK 提供者与 App 开发者开展合作前，需要通过服务协议或专门的安全协议，明确双方在个人信息保护及数据安全方面各自承担的义务和责任，特别是明确 App 开发者有义务通过隐私政策等形式明确告知个人用户第三方 SDK 收集个人信息的类型、目的、使用规则等，并获得个人用户同意。此外，第三方 SDK 提供者还可以建立对 App 开发者在合作前的数据合规尽职调查机制、合作过程中的合规巡查监测机制，以及对于未履行数据合规义务的 App 开发者，尽快采取行动要求改正或终止合作。

三是完善网络安全和数据安全防护措施。第三方 SDK 提供者在提供服务的过程中对个人信息的处理可以分为数据采集阶段、数据传输阶段、数据存储阶段、数据使用阶段以及数据销毁阶段。在每一阶段，第三方 SDK 提供者都需采取相应的技术措施以保障个人信息的安全，防止个人信息泄露或滥用风险。例如，在数据采集阶段，可以采用数据隔离、加密等方式保障缓存在终端本地的数据安全；在数据传输、存储阶段，采用数据隔离、加密、去标识化等方式降低因数据泄露造成的用户损失，尽量按照最小化原则保存个人信息；在数据使用阶段，尽量消除个人信息的身份指向性，避免精准定位到特定个人，加强展示时的脱敏处理以及个人信息访问控制管理；在数据销毁阶段，及时响应个人用户要求以及 App

开发者代表个人用户发出的数据删除的请求。此外，第三方 SDK 提供者还需要采取必要措施保障基础设施、业务系统等方面的网络安全，完善安全应急响应机制和应急预案，防范因黑客攻击造成数据泄露等安全风险，同时强化自身安全事件应急处置能力。

（四）加快研究制定 SDK 安全标准及指南

从目前已发布的国家标准及行业标准来看，针对移动应用软件（即 App），已经有了相对完整、成熟的个人信息保护技术要求、检测要求等标准，而对 SDK 安全关注较少。鉴于本报告第二章提及的第三方 SDK 安全问题逐步显现，建议尽快研究制定 SDK 开发安全、SDK 嵌入安全、恶意 SDK 识别与监测方法、SDK 安全评估及检测规范等方面的标准或指南，一方面帮助 App 开发者安全使用第三方 SDK，一方面指导第三方 SDK 提供者提升 SDK 安全性。

（五）鼓励第三方 SDK 企业开展行业自律

SDK 技术发展日新月异，第三方 SDK 安全问题也逐渐成为各方关注的焦点问题，建议鼓励相关 SDK 企业同步开展行业自律，作为立法与监管等国家公权力的补充力量，充分发挥专业性、经济型、灵活性等优势，共同营造 SDK 发展的良好生态。一方面，鼓励 SDK 企业自发或依托相关行业协会、社会组织平台，共同制定第三方 SDK 收集使用个人信息行为准则，签订行业自律公约，形成行业自治。另一方面，对当下法律规定不完善之处以及随着技术发展可能带来的全新问题，鼓励 SDK 企业共同探索安全实践和合规参考指南，推广宣传相关最佳实践，带动提升个人信息保护整体水平。

附录　第三方 SDK 产品的安全与合规实践

（一）极光 SDK 的安全与合规实践

1、SDK 开发者协议和隐私政策

（1）对开发者的要求

极光在其网站公布隐私政策，同时在极光用户注册界面展示隐私政策，访问者需同意极光开发者协议和隐私政策后才能成为极光开发者用户。极光在其隐私政策中明确说明了其为开发者提供服务的前提，包括但不限于（1）开发者已经遵守并将持续遵守适用的法律、法规和监管要求，包括但不限于制定和公布有关个人信息保护和隐私保护的相关政策；（2）如涉及需收集、存储、使用、共享来自于终端用户的个人信息，App 开发者须确认并承诺：其已经获得终端用户充分必要的授权、同意和许可；（3）开发者 App 应向终端用户提供易于操作的选择机制，说明终端用户如何以及何时可以行使选择权，并说明行使选择权后如何以及何时可以修改或撤回该选择，使得终端用户可以选择同意或不同意为互联网定向广告目的而收集和使用其身份关联信息以及向第三方共享该信息。极光通过站内信、网站形式不时更新或发布极光合规指南、向 App 开发者提供隐私政策、使用方式以及参考模板，以帮助开发者避免因违反相关法律法规遭受损失。

（2）技术保障措施

极光非常注重终端用户的个人信息安全。极光通过物理安全、安全技术、安全管理等措施审慎保护终端用户的个人信息，防止丢失、误用、非授权存取、泄露和非授权更改。安全措施包括但不限于防火墙、信息加密、数据备份、访问权限控制、密级管理、雇员保密协议和安全管理制度。极光会定期和不定期举办信

息安全和隐私保护培训课程，加强员工对于保护终端用户个人信息重要性的认识。

从数据处理生命周期角度来看，极光作为 SDK 提供者在提供服务过程中对个人信息的处理分为数据采集阶段、数据传输阶段、数据存储阶段、数据使用阶段、数据处理阶段。每一个阶段极光推送 SDK 均采取了相应的技术措施以保障终端用户个人信息的安全性，防止终端用户个人信息泄露。

2、标识用户方法及安全措施

数据在进入极光统计平台后，将进行匿名化工作，在个人信息第一次上报，通过系统的注册服务，结合设备标识与 App 标识，根据固定的算法加工生成 JID（极光唯一标识符）。通过 JID 与业务数据关联，在后续的业务使用过程中完全使用 JID 作为数据完整生命周期的标识。

3、数据存储安全措施

数据经客户端传输上报至服务端并经过缓存处理后，统一存储至统计平台待分析处理。存储时按照上报 App 进行单独隔离，个人信息与业务数据隔离存储，通过上述提及的 JID 作为关联 ID，防止存储数据泄露之后的可逆操作，保证了数据安全。除此之外极光采取严格的数据访问控制，采用独立的鉴权方式，按需申请达到针对个人的最小化权限控制，防止人为操作原因导致的数据泄露。

4. 数据汇聚

极光推送 SDK 为提供推送服务而收集到的各个 App 数据，在数据传入统计平台后，会依据不同 App 进行存储隔离，以保证数据的安全性。同时进入统计平台的数据，会依据不同的业务类型进行分级管理及存储，以保证相关人员对数据的最小可见。

数据依托极光 JID，对 SDK 收集的原始数据进行归类汇聚，并为客户提供基于时间、平台、客户自定义分类的归类和处理，处理完成后以网页呈现统计汇总及专属应用程序接口等方式提供给开发者，帮助开发者据此调整运营策略。

5、数据删除环节的主要做法

极光对缓存数据进行周期性归档，周期由 App 开发者选择设置（30/90/180 天）。如约定的周期已过或不再需要使用，超过该周期的推送业务 RID 对应的数据将自动归档处理。按照国家相关要求，日志信息需要保存 6 个月，之后归档数据将自动删除。

极光直接服务对象是开发者，并不直接面对终端用户。极光支持终端用户行使删除权利的途径有两种：（1）终端用户须提供其合法途径获得的独立权利要求证明文件，极光可能会要求进行身份验证，在向 App 开发者核实并且保障开发者账户安全的前提下，极光响应终端用户的相关请求；（2）根据 App 开发者的隐私政策，终端用户可以将与其个人信息相关的请求直接发送给相关 App 开发者处理和寻求帮助。

6. 对外合作情况

极光推送不向任何第三方提供能够单独或结合其他信息识别到终端用户个人身份的信息，也不允许任何第三方以任何形式访问这些数据。极光推送提供的用户和推送统计功能所形成的“推送报表”和“用户统计报表”，仅供开发者用来观察推送的效果和应用的发展趋势，不涉及终端用户的个人信息。同时，我们基于开发者服务协议合法收集的数据（对个人信息进行去标识化或匿名化处理）以及通过其他合法渠道获得的数据建立极光数据库，为开发者提供进一步的数据

服务。数据服务中我们输出的数据仅为标签信息，该等标签信息是通过海量移动端受众数据的汇聚、匿名化处理、智能运算获得，最终以统计分析数据的形式体现，不含有任何个人的隐私或可识别个体的内容。

7、新技术研发

极光认证整合了通信运营商的网关认证能力，为开发者提供一键登录和号码认证功能，优化用户注册/登录、号码验证的体验，提高安全性。使用极光认证，将登录过程从传统的 60 秒降低至 1~2 秒，极大提升用户体验。和短信验证码登录相比，极光认证的一键登录可有效降低短信验证码被劫持的风险；相对于传统密码登录方式而言，极光认证一键登录能避免账户密码泄露的风险；和第三方账号登录的形式相比，极光认证一键登录能一定程度上避免关联用户个人信息被泄露的风险。

（二）小米推送 SDK 的安全与合规实践

1、SDK 开发者协议和隐私政策

（1）对开发者的要求

小米在其开发者协议中，设立专门的隐私保护章节，规范开发者对终端用户的个人信息保护。要求开发者或终端用户在使用小米推送提供的服务时，同意小米推送按照小米统一隐私政策收集、存储、使用、披露和保护个人信息。小米也强烈建议开发者按照小米推送建议，将关键条款（具体以网页公示为准）包含进开发者产品面向终端用户的隐私政策中，并保证链接准确有效，即开发者应保证事先获得终端用户同意以使小米推送有权收集并使用数据提供相应服务。如果终端用户未作出同意，则开发者不应继续使用小米推送服务。小米还要求开发者同意遵守适用的收集、使用、披露终端用户数据及保护终端用户相关的法律法规、政策和行业标准，并确保符合该等法律法规、政策及行业标准的规定适用小米推送服务。作为小米推送服务的使用者，开发者必须制定、发布其隐私政策并获得终端用户同意，且该政策应不低于小米推送的隐私保护标准。

小米推送开发者上线界面中会明示开发者阅读并公示开发者隐私政策，并确保将推送所收集的信息部分集成进隐私政策中。开发者上线时须完成上述流程。

（2）技术保障措施

小米推送是小米开发的，被集成于开发者产品或服务中，用于为用户提供推送服务的产品。在此场景中，开发者作为数据控制者决定用户数据的处理目的、方式，小米推送在为用户提供推送服务过程中作为数据处理者，接受开发者委托并根据开发者指示处理用户数据。

小米非常重视个人信息安全，并采取一切合理可行的措施保护终端用户的个

人信息。我们会采用符合业界标准的安全防护措施以及行业内通行的安全技术来防止终端用户的个人信息遭到未经授权的访问、修改,避免您的个人信息泄露、损坏或丢失。个人信息全都被储存在安全的服务器上 ,并在受控设施中受到保护。我们依据重要性和敏感性对您的数据进行分类 ,并且保证您的个人信息具有相应的安全等级。同样，我们对以云为基础的数据存储设有专门的访问控制措施，我们定期审查信息收集、储存和处理实践，包括物理安全措施，以防止任何未经授权的访问和使用。

小米作为国内首家获得国际知名隐私认证机构 TrustArc 认证的公司，公司的管理制度、数据安全保护措施等均获得国际认可。

2、标识用户方法及安全措施

小米推送使用 regId 来唯一地标识一台设备上的一个应用(app)。 regId 是 app 在初始化小米推送 SDK 时， 由 SDK 从服务器端获取的一个 base64 编码的字符串。此字符串是由（数字，应用 AppID, 时间戳，数据中心编码）加密而成。不包含任何用户、设备相关的信息。

3、数据传输安全措施

消息在传递过程中， 使用 SSL 和 AES 二次加密的方式对内容进行保护。应用在初始化推送 SDK 时， 在注册设备阶段使用 HTTPS 方式与小米推送服务进行数据交换。此时，使用 SSL 对报文进行加密。此阶段会交换应用的 SecretKey, 做为下一阶段数据传输的公钥。

开发者向小米推送服务传递信息时，使用 HTTPS 来加密传输数据。小米推送服务向设备传递消息时，使用在注册阶段获得的 SecretKey, 对所有报文以 AES 128 bit 方式进行第一次加密。报文进入传输通道后，通道还会使用自己的通道加密方式对密文再次加密，确保数据安全。

4、数据使用情况

小米公司内部建立了完善的隐私数据保护管理制度。按照中国、欧盟、美国等各国法律规定，参考业界最佳实践，制定了以知情同意、目的限制、最少够用、数据质量、责任明确、公开透明、安全保障、提高用户信任感为基本原则。小米公司内部由专业的律师和隐私合规工程师评估小米推送的数据收集、使用等行为，确保符合法律规定、内部管理原则等。

小米推送服务只作为消息通道，将消息从开发者侧传递到设备侧。收集的数据只满足标识设备以下发消息和统计需求，承诺绝不未经用户同意对开发者提供的文本进行挖掘和使用，也不分析用户行为和偏好。

为改善整体服务质量，小米推送会对 App 和设备，以消息、时间维度进行统计。具体来说，每个 App 在一段时间内，对发起的请求数、送达数、点击数进行统计。统计结果是汇总数据，不对应到任何一个用户。

5、对外合作情况

小米推送的各类数据都没有提供给小米以外的合作方使用，包括原始数据、中间数据和统计结果，也不允许任何合作方在小米内部以任何形式访问这些数据。推送会为开发者提供与该开发者相关的后台统计数据，其中仅包括时间，消息维度的统计数据，不包括任何用户个人数据。

6、数据删除的主要做法

小米推送作为 SDK ,无界面与终端用户直接交互。用户相关信息的删除，都通过集成的 App 开发者来实施。小米推送 SDK 提供了反注册的方法和接口。调用此类方法，推送服务会将此 App 相关的数据和消息从数据库中删除。

当一台设备（以 UUID 标识）90 天都没有连接推送系统的记录，此设备相关的信息和消息，也会从数据库中删除掉。

除法律法规另有规定 ,未能下发的推送文本会在服务器中默认缓存十四日后清除，其余信息，自开发者停止集成小米推送 SDK、要求推送停止服务时，小米推送会根据开发者指示清除所有个人信息。

（三）TalkingData SDK 的安全与合规实践

1、SDK 开发者协议和隐私政策

TalkingData SDK 的功能设置为按需定制，开发者可以自主选择产品线、平台类型和定制化提供方式。开发者选择的 TalkingData 产品服务功能所需收集的信息类型与其自身的系统权限匹配。

开发者在 TalkingData 官网上获取 SDK 时须主动勾选所需的 SDK 功能并选择 App 上架的平台。

（1）对开发者的要求

TalkingData 在其《服务条款》中，明确了对开发者对个人信息保护的相关要求。开发者在使用 TallkingData 数据服务时，应同意其产品（包括但不限于移动应用客户端、移动网站、应用平台及其他 TalkingData 确认可供提供服务的其他终端等）中使用 TalkingData 分析工具，并且通过开发者和其产品用户的服务协议/软件许可条款或其他形式的许可或授权（“用户授权”），获得开发者产品用户的必要同意以使得 TalkingData 分析工具有权收集有关开发者产品使用情况的原始数据及其他为提供服务所必须的用户个人信息。

（2）技术保障措施

TalkingData 已经建立健全数据安全管理体系，包括对用户信息进行分级分类、加密保存、数据访问权限划分，指定内部数据管理制度和操作规程，从数据的获取、使用、销毁都有严格的流程要求，避免用户隐私数据被非法使用。

TalkingData 还建立了定期举办安全和隐私保护的培训机制，提高员工的个人保护意识。将不定期的审查、更新并公开 TalkingData 风险报告及个人信息安

全影响评估报告。

2、标识用户方法及安全措施

TalkingData SDK 基于分析服务所收集的数据，以及通过其他合法渠道获得的数据建立 TalkingData 数据库，通过汇聚、清洗、智能运算，形成 TalkingData 自有的用户标识符（TDID），来替代移动设备标识。TDID 采用 TalkingData 自有的 ID 生成逻辑及加密算法来生成，具体规则是：版本号 + 加密算法 F(设备 ID 因子 1,设备 ID 因子 2,设备 ID 因子 N, Salt)。

通过 SDK 在 App 第一次使用过程中所生成的 TDID，会保留在应用沙盒中（IOS 平台，对应存储于该应用自身的 Key Chain 中；Android 平台上，存储于应用自己的沙盒之中），从而确保 TDID 在设备端存储的安全性。

TalkingData 的 SDK 为每个 App 服务而收集的数据，首先在设备边缘侧先做了设备 ID 去标识化等预处理工作；收集的数据也采用加密方式存储和传输，通道加密方式回传。

3、数据存储安全措施

TalkingData 将采用行业内通行的、合理的标准来保护其所储存的信息的安全性和保密性。包括但不限于：防火墙和数据备份措施；数据中心的访问权限限制；对移动终端的识别性信息进行加密处理等。

TalkingData SDK 所收集的数据，用于对应的业务分析或广告监测业务服务线，并且在数据收集后，TalkingData 会按照“数据收集–存储–分析–利用–清理–归档”过程，严格追踪每一个数据使用的副本，在业务使用完成后，清除系统中所有相关的副本，同时，对需要保留的日志数据采用了包括：Hashing，映射、

设定数据偏移量、混淆、加密等各种脱敏技术方案，实现数据泛化，以有效保障数据的安全。

内部存储方面，依据“1. 法律法规；2. 行业规范；3.商业机密；4.资产安全”的四大原则，对收集后的数据进行分级存储和管理。

内部管理机制方面，也通过物理多级隔离控制（如：访问设备接入的身份验证、安全控制网关、服务使用的登录堡垒机隔离，以及数据使用的专属提交机）、账号分级管理、多层事后审计机制等手段，确保存储数据的操作安全。

图示：TalkingData 内部数据分级管理策略

4、数据汇聚安全措施

TalkingData SDK 为每个 App 服务而收集的数据，在数据回传通道中，首先依据不同国家和地区，采用分地区落盘存储方式，确保数据收集符合当地法律法规政策。

进入内部的数据，依据不同产品业务服务、不同客户的数据也按照公司的数据分级管理体系，进行分级化存储和管理。

借助 TalkingData 设备标识 TDID，针对 SDK 收集回的原始数据进行归类，并基于时间、产品服务业务线及客户等进行分主题归类和预处理，预处理完成后，按照具体业务需求，以统计汇总、专属应用程序接口等方式供给开发者使用。

5、数据使用安全措施

在 TalkingData 的数据中心内部，所有涉及数据使用的生产与治理全面采用了工具化方式管理，涵盖从研发工程(代码/配置/部署/任务/知识)、到生产领域(ETL)、数据资产管理、数据探索、及数据服务能力的使用及输出。

图示：数据生产/加工/访问使用全流程工具化操作

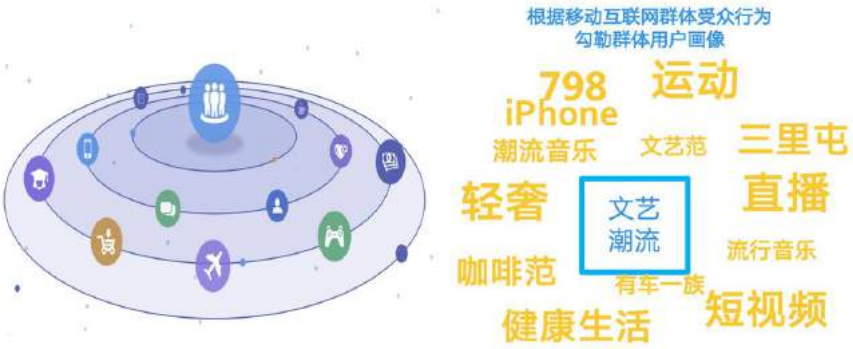
通过工具化手段，杜绝数据处理中的人工参与，整个处理和使用流程通过系统来做到安全管控和事后审计监督。

在内部数据探索方面，TalkingData 也构建了数据沙箱运行环境，通过构建数据探索使用的安全沙箱；在安全沙箱中，部署自有的数据科学平台（Data Science Studio），提供可视化建模工具，对存储于沙箱中的数据进行目录查阅，工程建模、模型调优的探索工作。

6、对外合作情况

在 SDK 数据服务能力对外服务提供方面，TalkingData 构建了移动端受众数据管理平台（TalkingData DMP 或称为 TalkingData 智能营销云），依托所累积和基于模型处理生产加工后所生成的第三方人群数据，这部分海量移动端受众数据的汇聚、匿名化处理，最终以统计分析数据形式展现，其中不包含任何个人信息和个人敏感性等可识性数据。通过受众管理平台提供客户群体构建、客群

画像洞察和画像群体对接媒体进行基于群体的定向投放的数据支撑。



图示：基于受众的群体画像能力输出

7、数据删除的主要做法

TalkingData SDK 收集的原始日志，基于国内法律规范，保留不少于 6 个月；业务使用过程中产生的数据副本，内部监控系统会时刻跟踪数据生产、加工处理过程中所产生的每一个数据副本，并依据事先的业务规则，在业务处理完成后，自动化删除每一个数据副本。

TalkingData 在为开发者提供的服务过程中或结束后，最终用户均可以通过 OPT-OUT 渠道 (http://www.talkingdata.com/optout.jsp?languagetype=zh_cn)随时向 TalkingData 提出撤回“同意”的申请，在收到申请后，TalkingData 将不再处理相应的信息，同时，可删除该申请用户在 TalkingData 账户下相关业务的所有统计分析数据。

8、新技术研发

TalkingData SDK 能力建设方面，主要关注智能化在终端侧的实现。主要包括：如何通过边缘结算和基于 AI 的模式识别能力，有效帮助开发者有效识别虚假作弊设备，帮助开发者判断设备使用，支持开发者统计和监测中的新模式分析等。

中国信息通信研究院安全研究所

地　　址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62305900

传　　真：010-62300264

网　　址：www.caict.ac.cn

北京市环球律师事务所

地　　址 :北京市朝阳区建国路 81 号华贸中心 1 号写字楼 15&20 层

邮政编码：100025

联系电话：010-65846688

传　　真：010-65846666

网　　址：www.glo.com.cn